

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C. 20505

OIS Registry

81-160/3

NSA review
completed

Reference: I-04123/81

24 AUG 1981

Mr. Arthur F. Van Cook
 Director of Information Security
 Office of the Deputy Under Secretary
 of Defense for Policy Review
 Department of Defense
 Room 3C260, Pentagon
 Washington, D.C. 20301

Dear Art:

We have reviewed the systematic classification review guidelines (DOD Directive 5200.30) transmitted by Mr. Stiver's memorandum of 12 February, and have made note of the suggestion to exchange guidance and the authorization to use this guidance to avoid the cost and time involved in referring documents for review. I am sorry to be so late with my response but it fell through a crack.

While recognizing the administrative advantages of such interchange, we feel we must decline the offer. Our experience has been that the sensitive aspects of many of our documents are sufficiently subtle or complex as to raise differences of viewpoint even among our experienced reviewers here as to their continuing classification status. Consequently, we would prefer to reserve these decisions to our own reviewers and components having jurisdiction over the material.

We have received, in the past year, a number of documents from various DOD components requesting a systematic review. We have attempted to handle all of these as expeditiously as possible. Should you have or become aware of complaints regarding our handling of these documents, please do not hesitate to let us know.

As you know, I will be departing for a sabbatical within the next few weeks. [redacted] will be acting in my behalf and can be reached at the same number [redacted] if you have need to discuss any topics of mutual concern.

Best regards,

/s/ Tom

Thomas H. White
 Director of Information Services
 Directorate of Administration

Distribution:

- Orig - Addressee
- 1 - OIS Subject
- 1 - OIS Chrono
- 1 - CRD Liaison w/DOD
- 1 - CRD Chrono

On file OSD release instructions

23 FEB 1981

MEMORANDUM FOR: Chief, Classification Review Division

FROM:

[Redacted]

Executive Officer, Office of Information Services

SUBJECT:

DoD Systematic Declassification Review Guidelines

1. The attached DoD memorandum provides the Agency with a copy of its systematic declassification review guidelines and grants the Agency authorization to apply the guidelines to DoD classified information in our files. It also requests that the DoD be authorized to apply our systematic declassification review guidelines to information held in DoD files that is under the classification review jurisdiction of the Agency.

2. You will note that the memorandum is directed to the Director of Administration and that it has been forwarded to OIS for action. Would you please prepare a response to DoD for DIS signature.

[Redacted]

STAT

Attachment

THE DEPARTMENT OF DEFENSE

WASHINGTON, D. C. 20301

81-0337

OIS Registry

81-160



POLICY REVIEW

12 FEB 1981

In reply refer to:
I-04123/81

MEMORANDUM FOR Director of Administration
Central Intelligence Agency

SUBJECT: Systematic Declassification Review Guidelines

Executive Order 12065, "National Security Information" requires that agency systematic declassification review guidelines be authorized for use by the Archivist of the United States and provides that such guidelines may be used by any other agency with approval of the issuing authority.

In the interest of improving the economic operation of the systematic declassification review process, I hereby authorize your Agency to apply our systematic declassification review guidelines to DoD classified information held in your files. A copy of our guidelines, which are a part of DoD Directive 5200.30, "Guidelines for Systematic Review of 20-Year-Old Classified Information in Permanently Valuable DoD Records," is enclosed for your use.

I am convinced that it would be mutually advantageous for agencies and departments of the Executive Branch to exchange systematic declassification review guidelines and to authorize their use by others. Such action can reduce the amount of documents referred for review and result in a cost avoidance for all concerned.

Accordingly, it is requested that the Department of Defense be authorized to apply your systematic declassification review guidelines to information held in DoD files that is under the classification jurisdiction of the Central Intelligence Agency.

Please contact Mr. Arthur F. Van Cook, my Director of Information Security, in the event that you have any questions concerning this matter.

A handwritten signature in black ink, reading "Ronald H. Stivers".

Ronald H. Stivers
Acting

Enclosure -
DoD Directive 5200.30

Approved For Release 2007/11/05 : CIA-RDP85B00236R000200170007-8

Feb 19 3 52 PM '81

Approved For Release 2007/11/05 : CIA-RDP85B00236R000200170007-8



June 18, 1979
NUMBER 5200.30

USD(P)

Department of Defense Directive

SUBJECT Guidelines for Systematic Review of 20-Year-Old
Classified Information in Permanently Valuable
DoD Records

References: (a) Secretary of Defense Memorandum, "Declassifi-
cation of World War II Records," May 3, 1972
(hereby canceled)
 (b) Deputy Secretary of Defense Memorandum,
 "Downgrading and Declassification of Histori-
cal Records," April 12, 1974 (hereby canceled)
 (c) Executive Order 12065, "National Security
Information," June 28, 1978
 (d) through (h), see enclosure 1

A. PURPOSE

This Directive reestablishes the policies contained in references (a) and (b); establishes guidelines for the systematic declassification review of 20-year-old information classified under references (c) through (f) and prior orders, directives and regulations governing security classification; implements section 3-402 of reference (c); and delegates authority to implement the DoD systematic declassification review guidelines.

B. APPLICABILITY AND SCOPE

1. The provisions of this Directive apply to the Office of the Secretary of Defense and to activities assigned for administrative support, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. This Directive applies to the systematic review of 20-year-old permanently valuable classified information, material, or records developed by or for the Department of Defense and its Components, or its predecessor components and activities, that are under the exclusive or final original classification jurisdiction of the Department of Defense. Accordingly, information that is foreign government information; Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954; or in nonpermanent records is outside the scope of this Directive.

C. DEFINITIONS

1. Cryptologic Information. Information pertaining to the activities and operations involved in the production of signals intelligence or to the maintenance of communications security.

2. Intelligence Method. Any human or technological method that is or may be used to collect or analyze foreign intelligence or foreign counterintelligence.

3. Intelligence Source. Any human or technological source from which foreign intelligence or foreign counterintelligence is, has been, or may be derived.

4. Foreign Government Information. Information that is provided to the United States by a foreign government or international organization of governments in the expectation, expressed or implied, that the information is to be kept in confidence; or produced by the United States pursuant to a written joint arrangement with a foreign government or international organization of governments requiring that either the information or the arrangement, or both, be kept in confidence. Such a written joint arrangement may be evidenced by an exchange of letters, a memorandum of understanding, or other written record.

D. POLICY AND PROCEDURES

1. DoD classified information that is permanently valuable, as defined by 44 U.S.C. 2103 (reference (g)), shall be systematically reviewed for declassification when it is 20 years old whether the information:

a. Has been transferred to the General Services Administration for accession into the Archives of the United States or in the possession and control of the Administrator of General Services under 44 U.S.C. 2107 or 2107 note (reference (h)), or

b. Is in the possession or control of DoD Components.

2. The transition to systematic review at 20 vice 30 years shall be implemented as rapidly as possible, and completed by December 1, 1988.

3. When DoD classified information becomes 20 years old, it shall be:

a. Declassified automatically if it is not within one of the categories specified in enclosure 2.

b. Reviewed for declassification by responsible DoD reviewers in accordance with enclosure 3 if it is within any of the categories specified in enclosure 2.

Jun 18, 79
5200.30

4. Systematic review for declassification shall be in accordance with procedures contained in DoD 5200.1-R (reference (f)). Information that falls within any of the categories in enclosure 2 shall be declassified if the designated DoD reviewer determines, in light of the declassification considerations of enclosure 3, that classification is no longer required. In the absence of such a determination, the designated DoD reviewer shall recommend continued classification in accordance with the procedures of reference (f).

E. RESPONSIBILITY AND AUTHORITY

1. The Deputy Under Secretary of Defense for Policy Review shall:

a. Exercise oversight and policy supervision over the implementation of this Directive;

b. Request DoD Components to review enclosures 2 and 3 of this Directive every 2 years;

c. Revise enclosures 2 and 3 to ensure they meet DoD needs; and

d. When appropriate, authorize other departments and agencies of the Executive Branch to apply the guidelines of this Directive to DoD information in their possession.

2. The Head of each DoD Component shall:

a. Recommend changes to enclosures 2 and 3 of this Directive;

b. Propose, with respect to specific programs, projects, and systems under their classification jurisdiction, supplements to enclosures 2 and 3 of this Directive;

c. Ensure that the records of the Component that have not been accessioned by the Archivist of the United States and, upon request of the Archivist, those that have been accessioned are reviewed by DoD personnel designated for the purpose in accordance with this Directive; and

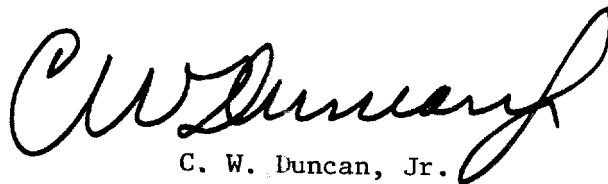
d. Provide advice and assistance to the Archivist of the United States in the systematic review of records under this Directive.

3. The Director, National Security Agency shall develop, for approval by the Secretary of Defense, special procedures for systematic review and declassification of classified cryptologic information.

4. The Archivist of the United States is authorized to apply this Directive when reviewing 20-year-old DoD classified information that has been accessioned into the Archives of the United States.

F. EFFECTIVE DATE

The provisions of this Directive are effective immediately.



C. W. Duncan, Jr.
Deputy Secretary of Defense

Enclosures - 3

1. References
2. Categories of Information to be Reviewed for Declassification
3. Declassification Considerations

Jun 18, 79
5200.30 (Encl 1)

REFERENCES, continued

- (d) Information Security Oversight Office Directive No. 1 Concerning National Security Information, October 2, 1978 (43 FR 194)
- (e) DoD Directive 5200.1, "DoD Information Security Program," November 29, 1978
- (f) DoD 5200.1-R, "Information Security Program Regulation," December 1978, authorized by DoD Directive 5200.1, November 29, 1978
- (g) Title 44, United States Code, Section 2103
- (h) Title 44, United States Code, Section 2107

(2) Procedures and techniques for noise reduction pertaining to an individual ship's component.

(3) Vibration data relating to hull and machinery.

c. Operational characteristics related to performance as follows:

(1) Endurance and total fuel capacity.

(2) Tactical information, such as times for ship turning, zero to maximum speed, and maximum to zero speed.

2. All information that is uniquely applicable to nuclear-powered surface ships or submarines.

3. Information concerning diesel submarines as follows:

a. Ship silencing data or acoustic warfare systems relative to:

(1) Overside, platform, and sonar noise signature.

(2) Radiated noise and echo response.

(3) All vibration data.

(4) Seismic, magnetic (including AM), pressure, and UEP signature data.

b. Details of operational assignments, i.e., war plans, anti-submarine warfare (ASW), and surveillance tasks.

4. Sound Surveillance System (SOSUS) data.

5. Information concerning mine warfare, mine sweeping, and mine countermeasures.

6. Electronic countermeasures (ECM) or electronic counter-countermeasures (ECCM) features and capabilities of any electronic equipment.

7. Torpedo information as follows:

a. Torpedo countermeasures devices: T-MK6 (FANFARE) and NAE beacons.

b. Tactical performance, tactical doctrine, and vulnerability to countermeasures.

8. Design performance and functional characteristics of guided missiles, guided projectiles, sonars, radars, acoustic equipments, and fire control systems.

H. Information concerning or revealing escape, evasion, cover, or deception plans, procedures, and techniques.

I. Information that reveals sources and methods of intelligence, counterintelligence activities, identities of clandestine human agents, methods of special operations, and analytical techniques for the interpretation of intelligence data.

J. Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures, electronic counter-countermeasures) or related activities to include:

1. Information concerning or revealing nomenclatures, functions, technical characteristics, or descriptions of foreign communications and electronic equipment, its employment/deployment, and its association with weapon systems or military operations.

2. Information concerning or revealing the processes, techniques, operations or scope of activities involved in acquiring, analyzing, and evaluating the above information, and the degree of success obtained.

K. Cryptologic information (including cryptologic sources and methods) currently in use. This includes information concerning or revealing the processes, techniques, operations, and scope of signals intelligence comprising communications intelligence, electronics intelligence, and telemetry intelligence; and the cryptosecurity and emission security components of communications security, including the communications portion of cover and deception plans.

1. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

- a. Those that relate to communications security (COMSEC). In documentary form, they provide COMSEC guidance or information. Normally, COMSEC documents and materials are accountable under the "Communications Security Material Control System." Examples are: items bearing "TSEC" nomenclature ("TSEC" plus three letters), "Crypto Keying Material" for use in enciphering communications, Controlled COMSEC Items (CCI), and cryptographic keying devices.

- b. Those that relate to signals intelligence (SIGINT). These appear as reports in various formats that bear security classification, sometimes followed by a five-letter codeword (World War II's ULTRA, for example) and often carry warning caveats such as "This document contains codeword material," "Utmost secrecy is necessary...". Formats will appear, for example, as messages having addressees, "from" and "to" sections, and as

summaries with SIGINT content with or without other kinds of intelligence and comment.

c. Research, development, test, and evaluation reports and information that relate to either COMSEC or SIGINT.

2. Commonly used words that may help in identification of cryptologic documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signal intelligence" or "SIGINT," "signal security," and "TEMPEST."

Jun 18, 79
5200.30 (Encl 3)

DECLASSIFICATION CONSIDERATIONS

A. Technological developments; widespread public knowledge of the subject matter; changes in military plans, operations, systems, or equipment; changes in the foreign relations or defense commitments of the United States and similar events may bear upon the determination of whether information should be declassified. If the responsible DoD reviewer decides that, in view of such circumstances, the public disclosure of the information being reviewed would no longer result in at least identifiable damage to the national security, the information must be declassified.

B. The following are examples of considerations which may be appropriate in deciding whether information in the categories listed in enclosure 2 may be declassified when it is reviewed:

1. The information no longer provides the United States a scientific, engineering, technical, operational, intelligence, strategic, or tactical advantage over other nations.
2. The operational military capability of the United States revealed by the information no longer constitutes a limitation on the effectiveness of the armed forces.
3. Information pertinent to a system is no longer used or relied on for the defense of the United States or its allies.
4. The program, project, or system information no longer reveals a current weakness or vulnerability.
5. The information pertains to an intelligence objective or diplomatic initiative that has been abandoned or achieved, and will no longer damage the foreign relations of the United States.
6. The information reveals the fact or identity of a United States intelligence source, method, or capability that is no longer employed and that relates to no current source, method, or capability that upon disclosure could cause at least identifiable damage to national security or place a person in immediate jeopardy.
7. The information concerns foreign relations matters the disclosure of which can no longer be expected to cause or increase international tension to the detriment of the national security of the United States.

C. Declassification of information that reveals the identities of clandestine human agents shall only be accomplished in accordance

with procedures established by the Director of Central Intelligence for that purpose.

D. Special procedures of the National Security Agency apply to the review and declassification of classified cryptologic information. The following shall be observed in the review of such information:

1. COMSEC Documents and Materials. If records or materials in this category are found in agency or department files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency or department concerned or by appropriate channels to the following address:

Director
National Security Agency/Central Security Service
ATTN: D4/I
Fort George G. Meade, MD 20755

2. SIGINT Information.

- a. If the SIGINT information is contained in a document or record originated by a DoD cryptologic organization, such as the National Security Agency, and is in the files of a noncryptologic agency or department, such material will not be declassified if retained in accordance with an approved records disposition schedule.

- b. If the SIGINT information has been incorporated by the receiving agency or department into documents it produces, referral to the National Security Agency is necessary prior to any declassification action.

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

DoD Systematic Declassification Review Guidelines

FROM:

Executive Officer, Office of
Information Services
1206 Ames Building

EXTENSION

NO.

OIS 81-160/1

DATE

23 February 1981

TO: (Officer designation, room number, and building)

DATE

RECEIVED

FORWARDED

OFFICER'S
INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. Chief, CRD

24
Feb
81

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

FORM
1-79

610 USE PREVIOUS
EDITIONS